Automatically detect and support against anti-debug with IDA/Ghidra to streamline debugging process

Takahiro Takeda

Cyber Emergency Center, LAC

Profile

Takahiro Takeda

Malware Analysis Team

CYBER EMERGENCY CENTER

LAC

2016: Analysis work as a Security Analyst.
2017: Analyzing malware and logs, as well as investigating smishing.
2019: Mainly Responsible for malware analysis related to incidents.

Speaker Experience:
PACSEC, AVAR, HITCON, Black Hat USA Arsenal

Agenda

- What is AntiDebugSeeker
- Demo
  IDA version
- Introduction to Configuration Files
- Demo
  GHIDRA version
- Introduction to Files related to Ghidra Version
- Summary

What is AntiDebugSeeker

This is a program for automatically identify and extract potential anti-debugging techniques used by malware and displaying them in IDA / Ghidra.

The main functionalities of this plugin are as follows:

1. Extraction of APIs that are potentially being used for anti-debugging by the malware.

2. Using multiple keywords, anti-debugging techniques are extracted.

※For packed samples, running this plugin after unpacking and fixing the Import Address Table is more effective.

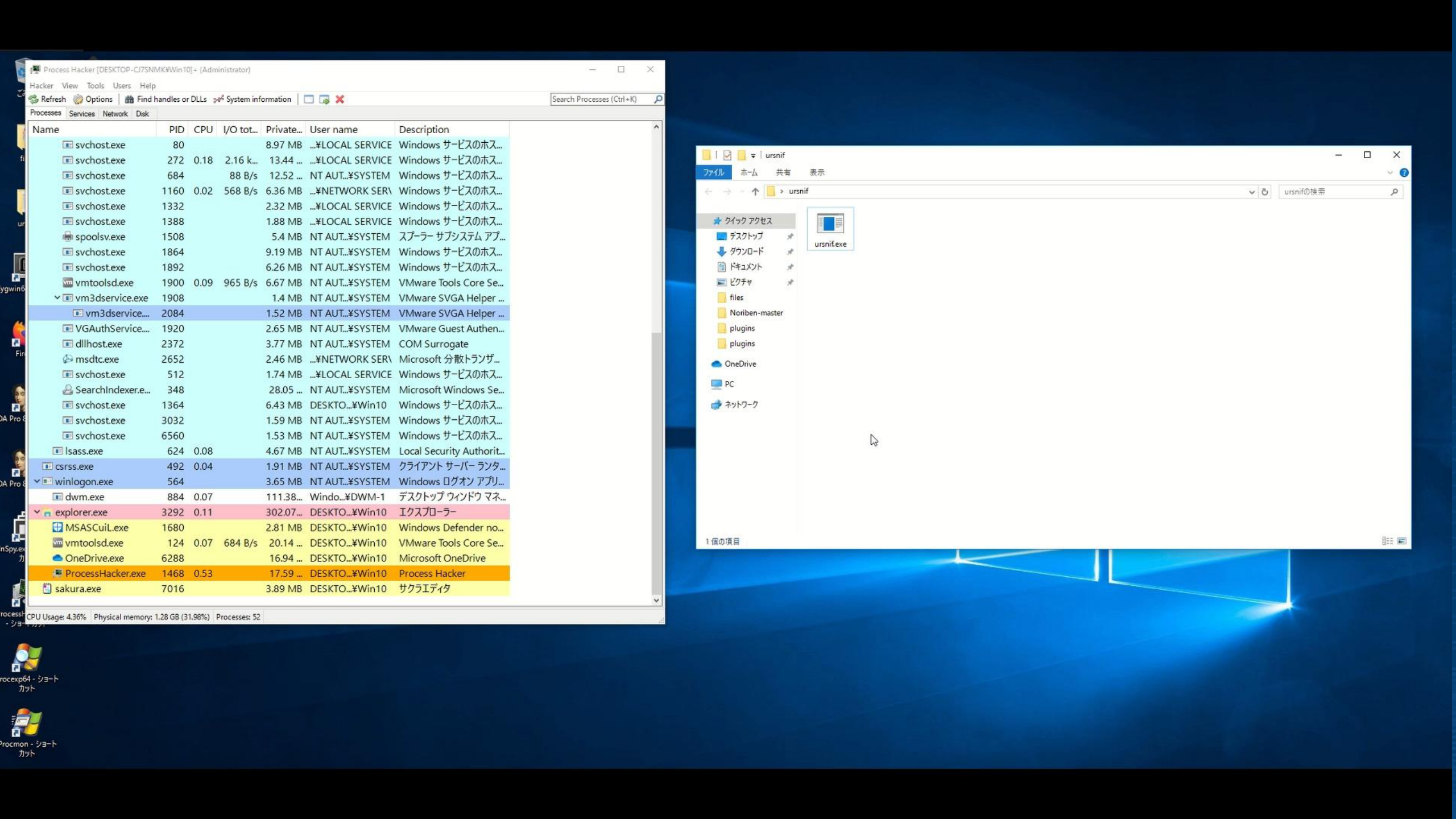
Demo: IDA version of AntiDebugSeeker

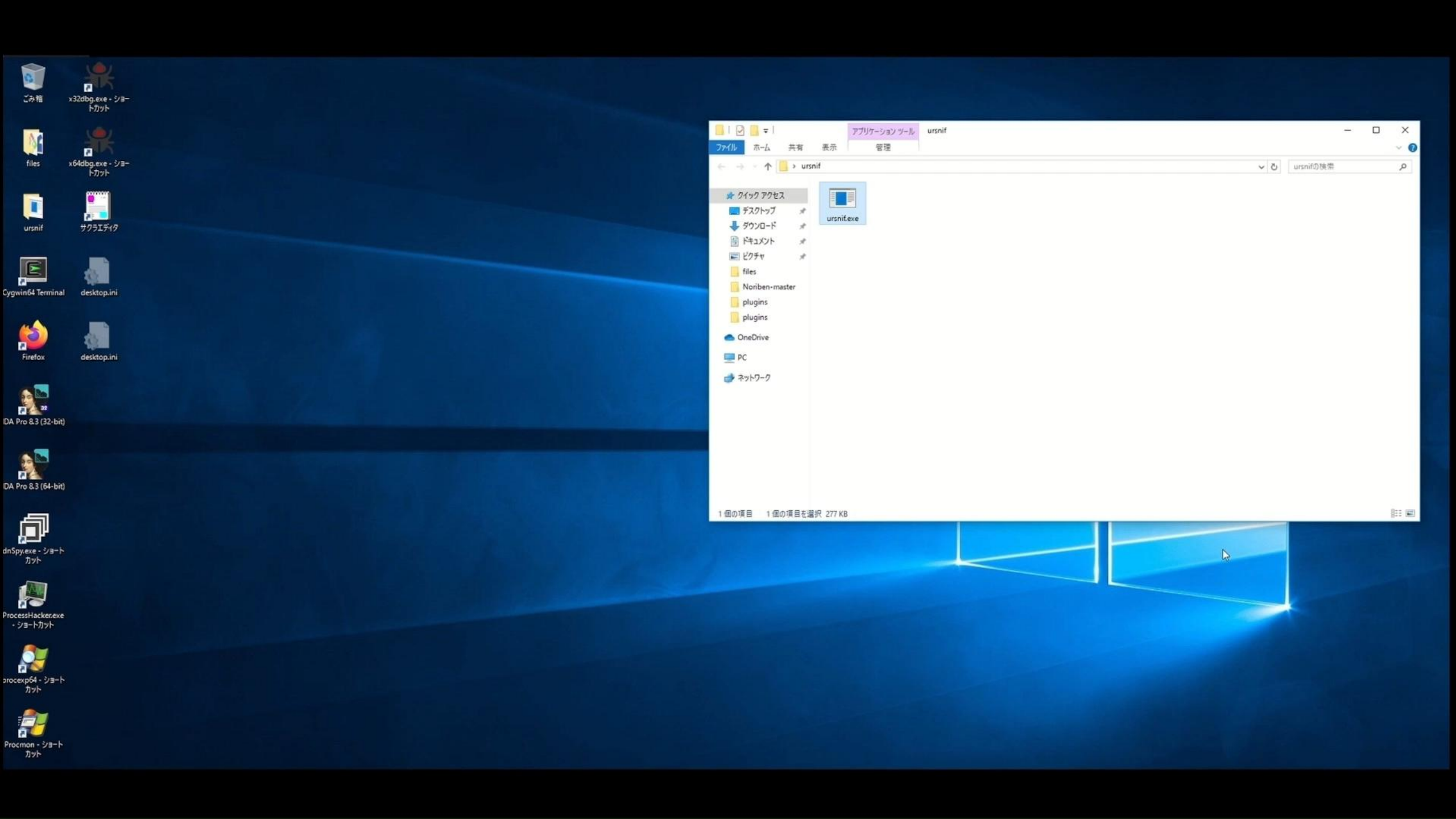
DEMO

Malware : Ursnif

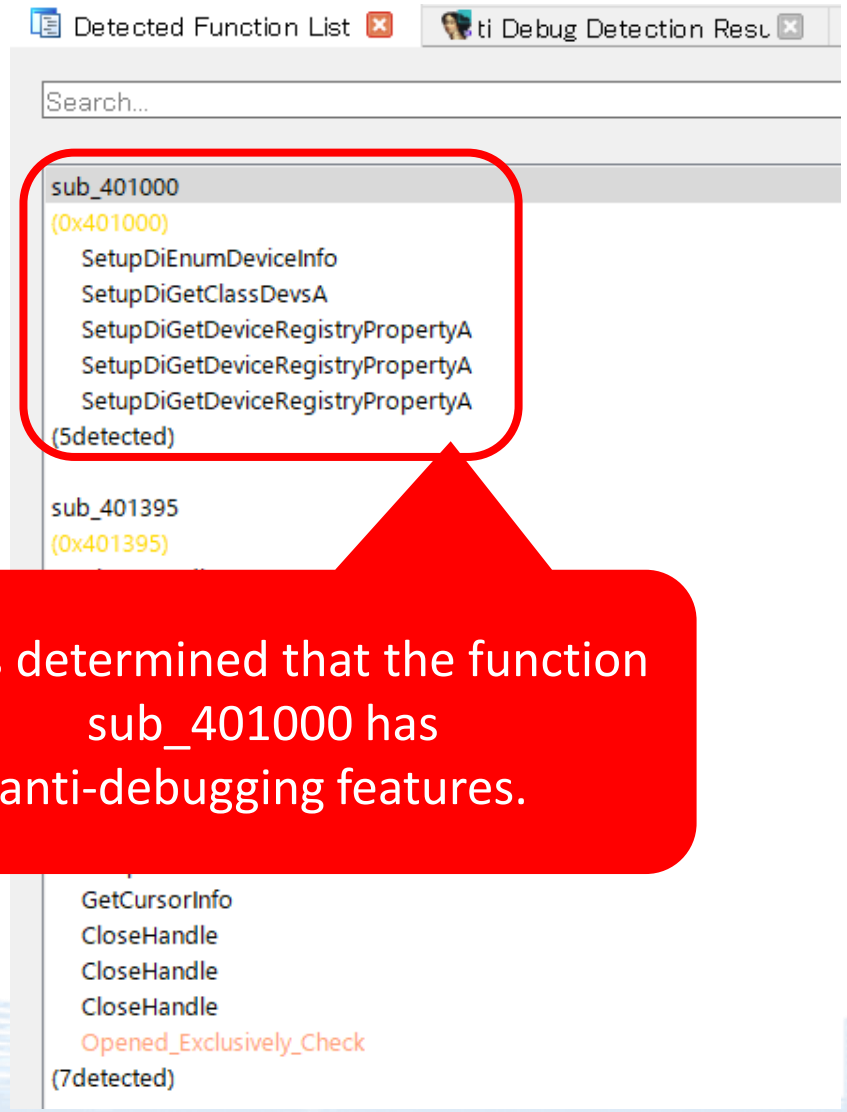
MD5 : 4da11c829f8fea1b690f317837af8387 (Packed)
MD5 : 952d604345e051fce76729ccb63bde82 (Unpack)

The flow of a demo
①A type of anti-analysis leads to the termination of the process.
②Using AntiDebugSeeker to find anti-analysis features.
③Apply patches using a debugger.

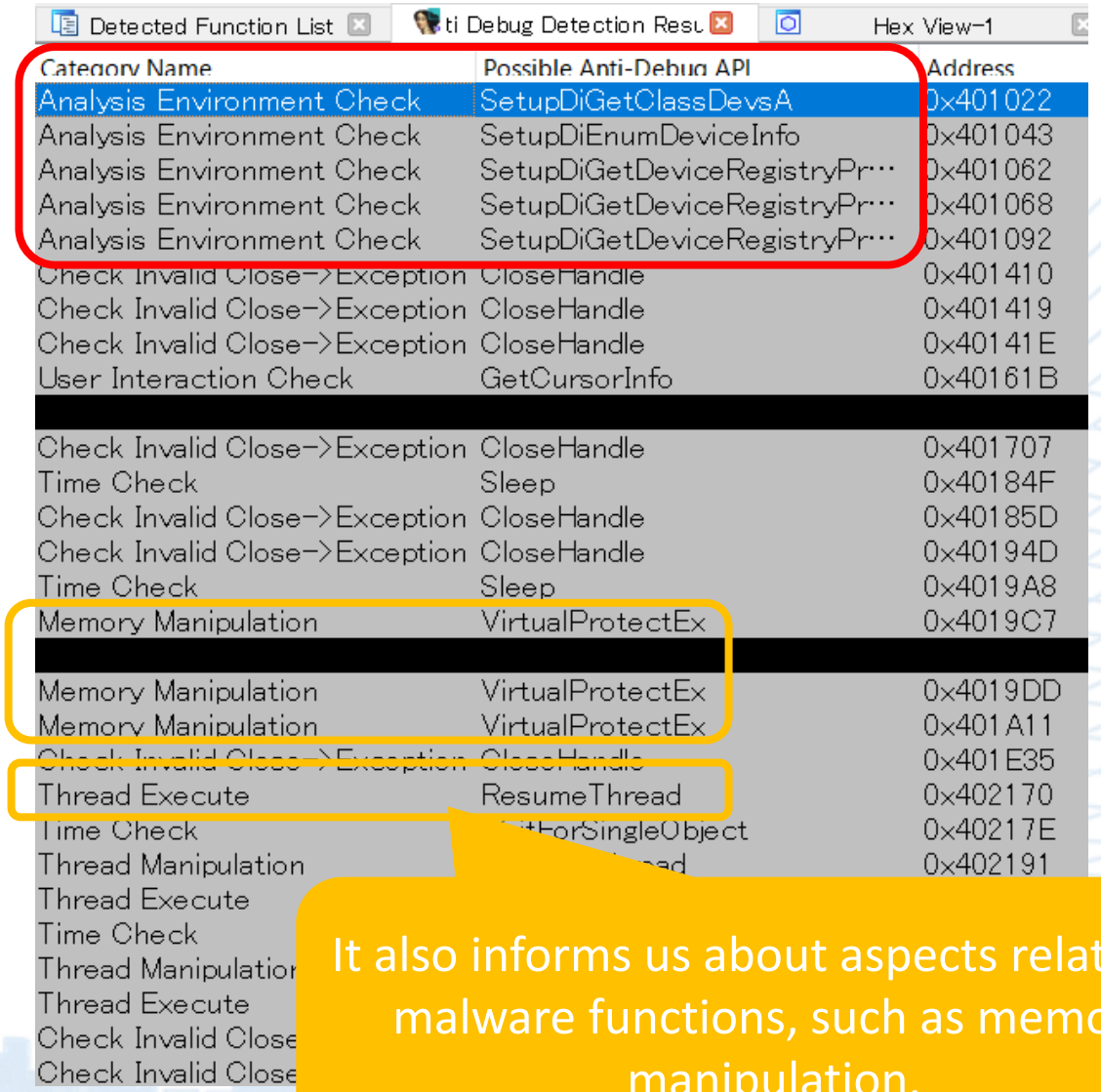

Process Hacker [DESKTOP-CJ7SNMK¥Win10]+ (Administrator)
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
Processes Services Network Disk
Name PID CPU I/O tot... Private... User name Description
svchost.exe 80 8.97 MB ...¥LOCAL SERVICE Windows サービスのホス...
svchost.exe 272 0.18 2.16 k... 13.44 ... ...¥LOCAL SERVICE Windows サービスのホス...
svchost.exe 684 88 B/s 12.52 ... NT AUT...¥SYSTEM Windows サービスのホス...
svchost.exe 1160 0.02 568 B/s 6.36 MB ...¥NETWORK SER\ Windows サービスのホス...
svchost.exe 1332 2.32 MB ...¥LOCAL SERVICE Windows サービスのホス...
svchost.exe 1388 1.88 MB ...¥LOCAL SERVICE Windows サービスのホス...
spoolsv.exe 1508 5.4 MB NT AUT...¥SYSTEM スプーラー サブシステム アプ...
svchost.exe 1864 9.19 MB NT AUT...¥SYSTEM Windows サービスのホス...
svchost.exe 1892 6.26 MB NT AUT...¥SYSTEM Windows サービスのホス...
vmtoolsd.exe 1900 0.09 965 B/s 6.67 MB NT AUT...¥SYSTEM VMware Tools Core Se...
vm3dservice.exe 1908 1.4 MB NT AUT...¥SYSTEM VMware SVGA Helper ...
vm3dservice.... 2084 1.52 MB NT AUT...¥SYSTEM VMware SVGA Helper ...
VGAuthService.... 1920 2.65 MB NT AUT...¥SYSTEM VMware Guest Authen...
dllhost.exe 2372 3.77 MB NT AUT...¥SYSTEM COM Surrogate
msdtc.exe 2652 2.46 MB ...¥NETWORK SER\ Microsoft 分散トランザ...
svchost.exe 512 1.74 MB ...¥LOCAL SERVICE Windows サービスのホス...
SearchIndexer.e... 348 28.05 ... NT AUT...¥SYSTEM Microsoft Windows Se...
svchost.exe 1364 6.43 MB DESKTO...¥Win10 Windows サービスのホス...
svchost.exe 3032 1.59 MB NT AUT...¥SYSTEM Windows サービスのホス...
svchost.exe 6560 1.53 MB NT AUT...¥SYSTEM Windows サービスのホス...
lsass.exe 624 0.08 4.67 MB NT AUT...¥SYSTEM Local Security Authorit...
csrss.exe 492 0.04 1.91 MB NT AUT...¥SYSTEM クライアント サーバー ランタ...
winlogon.exe 564 3.65 MB NT AUT...¥SYSTEM Windows ログオン アプリ...
dwm.exe 884 0.07 111.38... Windo...¥DWM-1 デスクトップ ウィンドウ マネ...
explorer.exe 3292 0.11 302.07... DESKTO...¥Win10 エクスプローラー
MSASCuiL.exe 1680 2.81 MB DESKTO...¥Win10 Windows Defender no...
vmtoolsd.exe 124 0.07 684 B/s 20.14 ... DESKTO...¥Win10 VMware Tools Core Se...
OneDrive.exe 6288 16.94 ... DESKTO...¥Win10 Microsoft OneDrive
ProcessHacker.exe 1468 0.53 17.59 ... DESKTO...¥Win10 Process Hacker
sakura.exe 7016 3.89 MB DESKTO...¥Win10 サクラエディタ
CPU Usage: 4.36% Physical memory: 1.28 GB (31.98%) Processes: 52
ursnif
ファイル ホーム 共有 表示
ursnif
ursnifの検索
クイック アクセス
デスクトップ
ダウンロード
ドキュメント
ピクチャ
files
Noriben-master
plugins
plugins
OneDrive
PC
ネットワーク
ursnif.exe
1 個の項目
procexp64 - ショートカット
Procmon - ショートカット


ごみ箱
x32dbg.exe - ショートカット
files
x64dbg.exe - ショートカット
ursnif
サクラエディタ
Cygwin64 Terminal
desktop.ini
Firefox
desktop.ini
IDA Pro 8.3 (32-bit)
IDA Pro 8.3 (64-bit)
dnSpy.exe - ショートカット
ProcessHacker.exe - ショートカット
procexp64 - ショートカット
Procmon - ショートカット
アプリケーション ツール
ursnif
ファイル
ホーム
共有
表示
管理
ursnif
ursnifの検索
クイック アクセス
デスクトップ
ダウンロード
ドキュメント
ピクチャ
files
Noriben-master
plugins
plugins
OneDrive
PC
ネットワーク
ursnif.exe
1 個の項目
1 個の項目を選択 277 KB

The Analysis result of IDA-AntiDebugSeeker



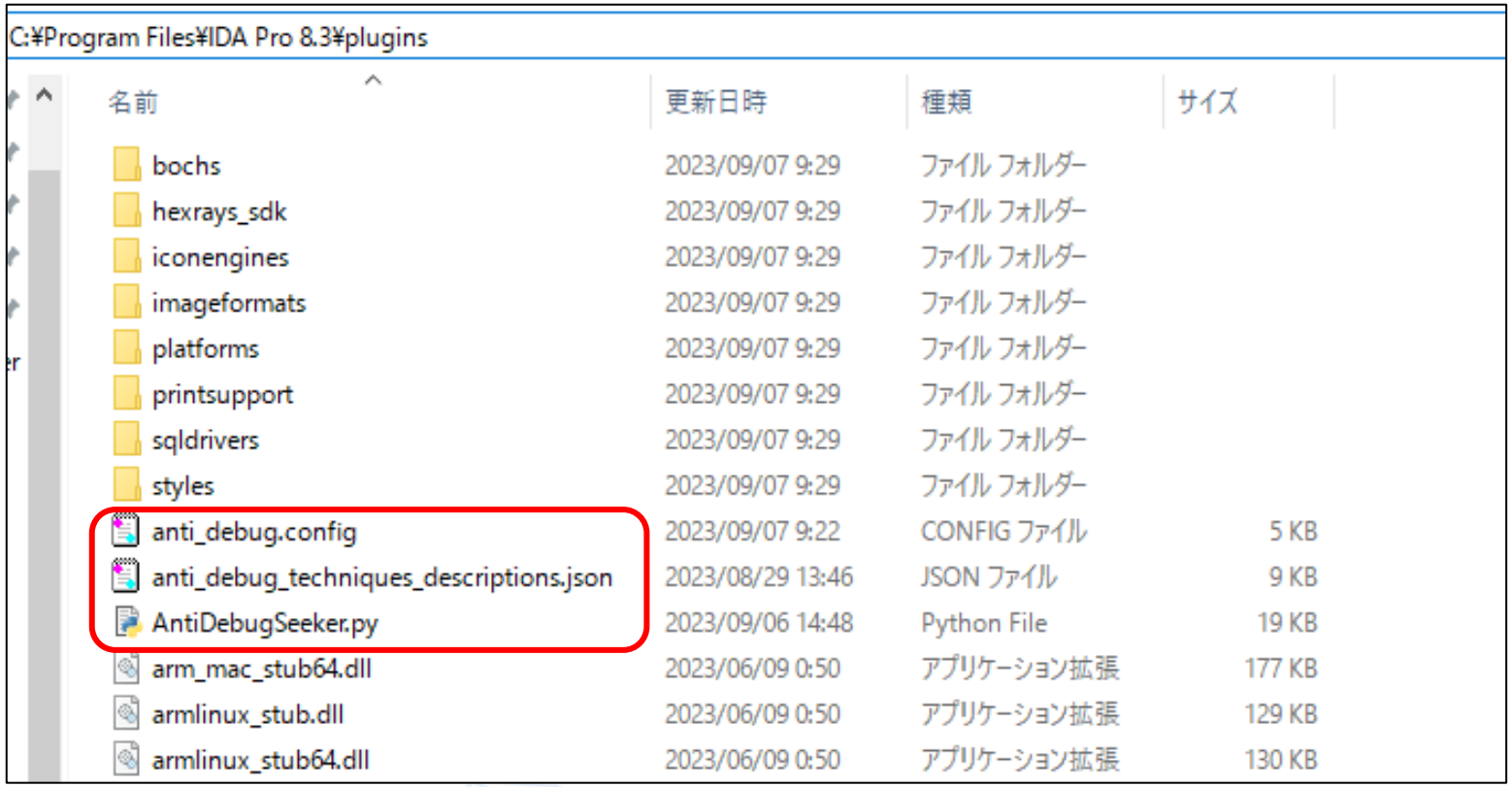
It was determined that the function sub_401000 has anti-debugging features.



It also informs us about aspects related to malware functions, such as memory manipulation.

Introduction to configuration files

Files Required to Run the Program



Please place the following three files under the plugin directory of IDA :

1.anti_debug.config (A file containing rules for detecting anti-debugging techniques)
2.anti_debug_techniques_descriptions.json (A file containing descriptions of the detected rules)
3.AntiDebugSeeker.py (The anti-debugging detection program)

anti_debug.config

Anti_Debug_API

```
###Anti_Debug_API###
[CommandLine check]
GetCommandLineA
GetCommandLineW

[Debugger check]
CheckRemoteDebuggerPresent
DebugActiveProcess
DebugBreak
DbgSetDebugFilterState
DbgUiDebugActiveProcess
IsDebuggerPresent
NtDebugActiveProcess
NtQueryObject
NtSetDebugFilterState
NtSystemDebugControl
OutputDebugStringA
OutputDebugStringW
```

In the Anti_Debug_API section, you can freely create categories and add any number of APIs you want to detect. (exact match)

```
###Anti_Debug_API###
[Category Name_1]
API1
API2
API3

[Category Name_2]
API4
API5
API6
```

anti_debug.config

Anti_Debug_Technique

```
###Anti_Debug_Technique###
default_search_range=80

[VMware_I/O_port]
5658h

[VMware_magic_value]
564D5868h

[HeapTailMarker]
ABABABAB

[KernelDebuggerMarker]
7FFE02D4

[DbgBreakPoint_RET]
DbgBreakPoint
C3h

[DbgUiRemoteBreakin_Debugger_Terminate]
DbgUiRemoteBreakin
TerminateProcess
```

You can set up to three keywords (partial match) under a single rule name.

```
###Anti_Debug_Technique###
default_search_range=80

[Rule1]
ABC
DEF
GHI
search_range=200
```

80bytes

80bytes

Search Target:

- Disassembly (Opcode, Operand)
- Comments
- API based on Import Table

anti_debug_techniques_descriptions.json

```
{
    "VMware_I/O_port" : "detect a VM environment based on the VMware I/O port",
    "VMware_magic_value" : "detect a VM environment based on the VMware magic valu
    "HeapTailMarker": "Malware can detect if it's on a debug heap by checking the                                    ABABABAB, i
    "KernelDebuggerMarker": "Detect Kernelmode Debugger(KdDebuggerEnabled)",
    "DbgBreakPoint_RET": "This detection may be due to the first byte of the DbgBr                                   C3, which co
    "DbgUiRemoteBreakin_Debugger_Terminate": "When a debugger tries to attach to a                                   inates.",
    "PMCCheck_RDPMC": "The RDPMC (Read Performance-Monitoring Counters) the value                                   MC) to deter
    "TimingCheck_RDTSC": "The RDTSC (Read Time Stamp Counter) instruction can be u                                   utilized in
    "Environment_TimingCheck_CPUID": "The CPUID instruction can be used as part of                                   volves check
    "SkipPrefixes_INT1":"This anti-debugging method exploits how some debuggers ha                                   ion prefixes
    "INT2D_interrupt_check": "The INT2D instruction either passes control to a deb                                   alue if no d
    "INT3_interrupt_check": "This is a debug detection mechanism using the INT 3 i                                   if the progr
    "EXCEPTION_BREAKPOINT": "This is a debug detection method using the INT 3 inst                                   e program is
    "ICE_interrupt_check": "If a program is debugged, the debugger sees the except                                   p bit in the
    "DBG_PRINTEXCEPTION_C": "This may involve anti-debugging by utilizing the DBG_                                   triggered by
    "TrapFlag_SingleStepException": "This anti-debugging technique utilizes the Tr                                   ecimal 100)
    "BeingDebugged_check" : "The BeingDebugged field in the Process Environment Bl                                   process is b
    "NtGlobalFlag_check": "The code is checking the NtGlobalFlag value at offset 0                                   \nThe value
    "NtGlobalFlag_check_2": "The code is checking the NtGlobalFlag value at offset                                   t Block. \nT
    "HeapFlags" : "HeapFlags stores various heap-related flags, bit by bit. \nThes                                   in features
```

Anti_Debug_Technique

```
###Anti_Debug_Technique###
default_search_range=80

[VMware_I/O_port]
5658h

[VMware_magic_value]
564D5868h

[HeapTailMarker]
ABABABAB

[KernelDebuggerMarker]
7FFE02D4

[DbgBreakPoint_RET]
DbgBreakPoint
C3h

[DbgUiRemoteBreakin_Debugger_Terminate]
DbgUiRemoteBreakin
TerminateProcess
```

Demo:
Ghidra version of AntiDebugSeeker

DEMO

Malware : Qakbot (aka. Qbot)

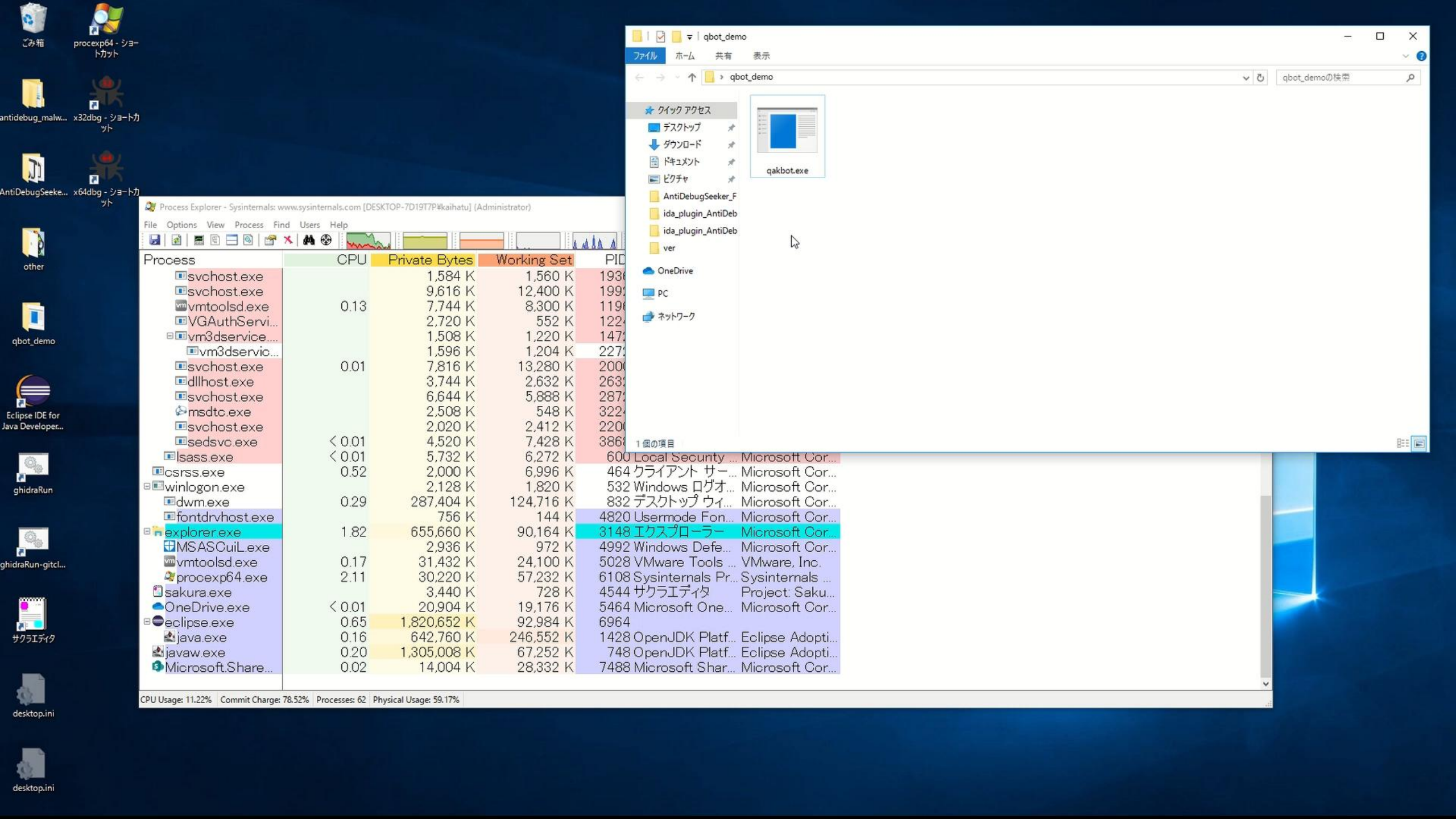
- MD5 : bce0df8721504d50f4497c0a0a2c090d (Packed)
- MD5 : 58e1c32eeb0130da19625e55ee48cf1e (Unpack)

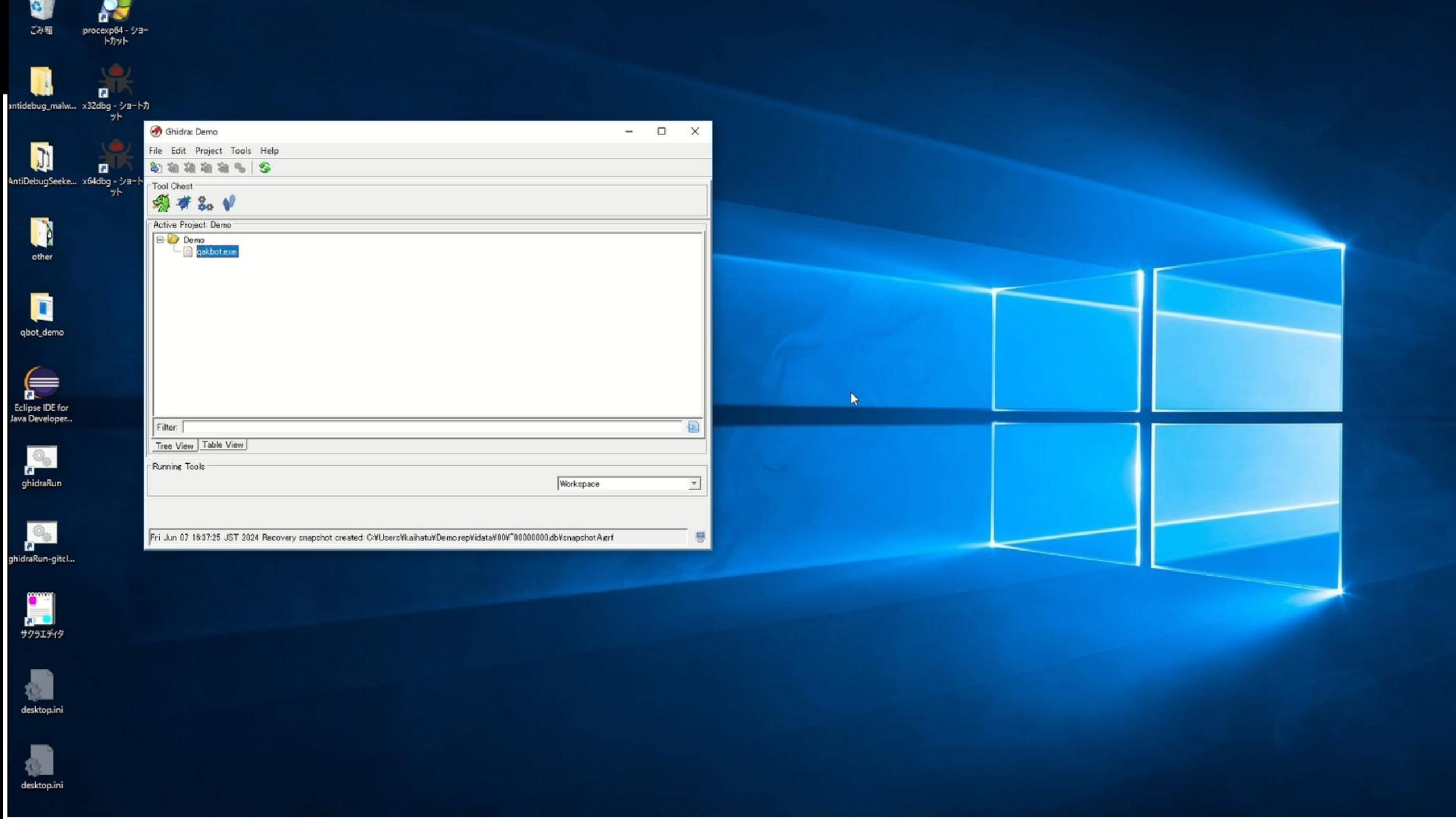
The flow of a demo

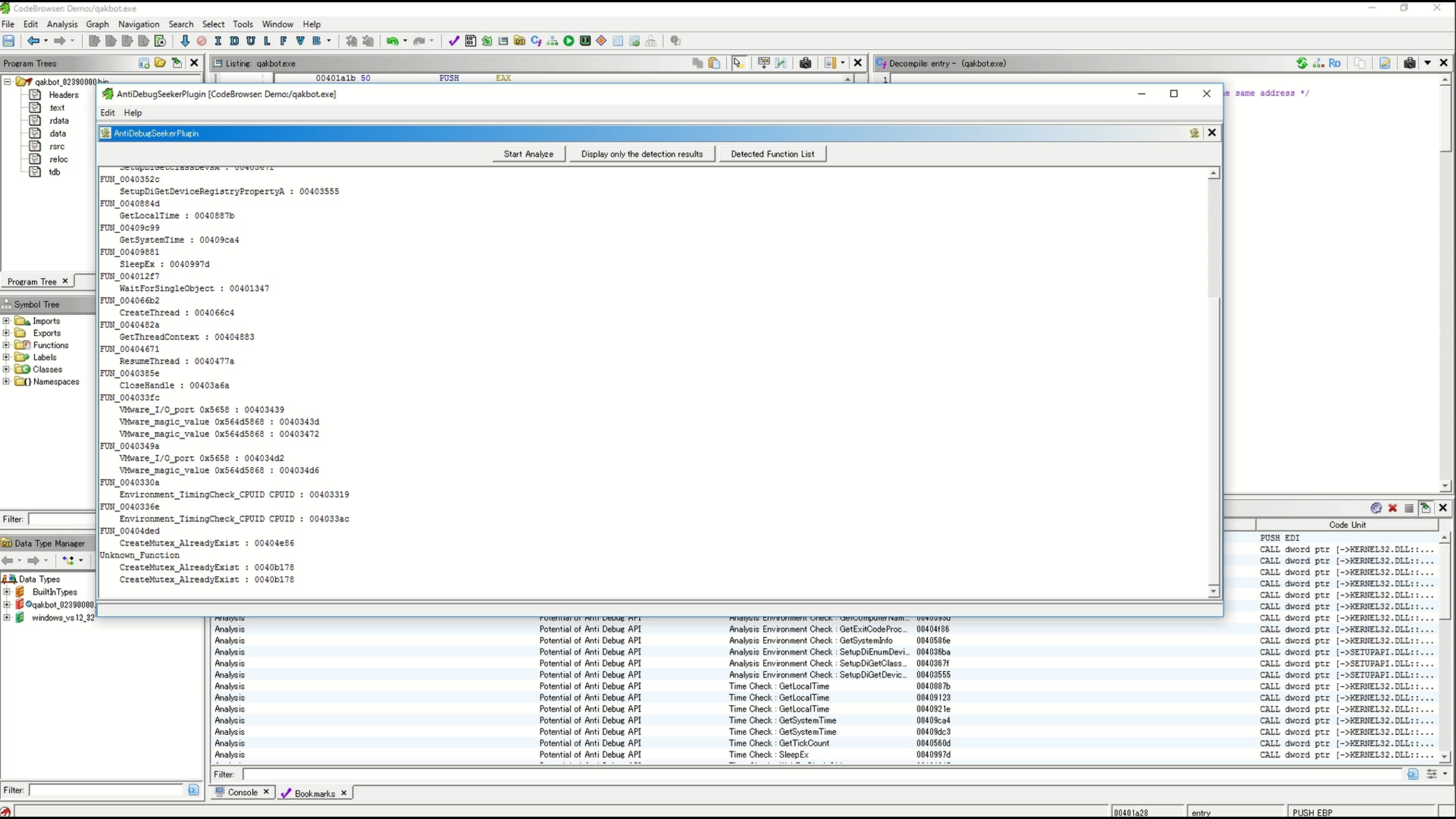
①A type of anti-analysis leads to the termination of the process.

②Using AntiDebugSeeker to find anti-analysis features.

③Examine the behavior of AntiDebug, and identify the areas to patch from the AntiDebugSeeker results + Apply the patch using a debugger.


ごみ箱
procexp64 - ショートカット
antidebug_malw...
x32dbg - ショートカット
AntiDebugSeeke...
x64dbg - ショートカット
other
qbot_demo
Eclipse IDE for Java Developer...
ghidraRun
ghidraRun-gitcl...
サクラエディタ
desktop.ini
desktop.ini
qbot_demo
ファイル
ホーム
共有
表示
qbot_demo
qbot_demoの検索
クイック アクセス
デスクトップ
ダウンロード
ドキュメント
ピクチャ
AntiDebugSeeker_F
ida_plugin_AntiDeb
ida_plugin_AntiDeb
ver
OneDrive
PC
ネットワーク
qakbot.exe
1 個の項目
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-7D19T7P¥kaihatu] (Administrator)
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID
svchost.exe 1,584 K 1,560 K 193
svchost.exe 9,616 K 12,400 K 199
vmtoolsd.exe 0.13 7,744 K 8,300 K 119
VGAuthServi... 2,720 K 552 K 122
vm3dservice.... 1,508 K 1,220 K 147
vm3dservic... 1,596 K 1,204 K 227
svchost.exe 0.01 7,816 K 13,280 K 200
dllhost.exe 3,744 K 2,632 K 263
svchost.exe 6,644 K 5,888 K 287
msdtc.exe 2,508 K 548 K 322
svchost.exe 2,020 K 2,412 K 220
sedsvc.exe < 0.01 4,520 K 7,428 K 386
lsass.exe < 0.01 5,732 K 6,272 K 600 Local Security ... Microsoft Cor...
csrss.exe 0.52 2,000 K 6,996 K 464 クライアント サー... Microsoft Cor...
winlogon.exe 2,128 K 1,820 K 532 Windows ログオ... Microsoft Cor...
dwm.exe 0.29 287,404 K 124,716 K 832 デスクトップ ウィ... Microsoft Cor...
fontdrvhost.exe 756 K 144 K 4820 Usermode Fon... Microsoft Cor...
explorer.exe 1.82 655,660 K 90,164 K 3148 エクスプローラー Microsoft Cor...
MSASCuiL.exe 2,936 K 972 K 4992 Windows Defe... Microsoft Cor...
vmtoolsd.exe 0.17 31,432 K 24,100 K 5028 VMware Tools ... VMware, Inc.
procexp64.exe 2.11 30,220 K 57,232 K 6108 Sysinternals Pr... Sysinternals ...
sakura.exe 3,440 K 728 K 4544 サクラエディタ Project: Saku...
OneDrive.exe < 0.01 20,904 K 19,176 K 5464 Microsoft One... Microsoft Cor...
eclipse.exe 0.65 1,820,652 K 92,984 K 6964
java.exe 0.16 642,760 K 246,552 K 1428 OpenJDK Platf... Eclipse Adopti...
javaw.exe 0.20 1,305,008 K 67,252 K 748 OpenJDK Platf... Eclipse Adopti...
Microsoft.Share... 0.02 14,004 K 28,332 K 7488 Microsoft Shar... Microsoft Cor...
CPU Usage: 11.22% Commit Charge: 78.52% Processes: 62 Physical Usage: 59.17%


ごみ箱
procexp64 - ショートカット
antidebug_malw...
x32dbg - ショートカット
AntiDebugSeeke...
x64dbg - ショートカット
other
qbot_demo
Eclipse IDE for Java Developer...
ghidraRun
ghidraRun-gitcl...
サクラエディタ
desktop.ini
desktop.ini
Ghidra: Demo
File Edit Project Tools Help
Tool Chest
Active Project: Demo
Demo
qakbot.exe
Filter:
Tree View
Table View
Running Tools
Workspace
Fri Jun 07 16:37:25 JST 2024 Recovery snapshot created: C:¥Users¥kaihatu¥Demo.rep¥idata¥00¥~00000000.db¥snapshotA.grf


CodeBrowser: Demo:/qakbot.exe
File Edit Analysis Graph Navigation Search Select Tools Window Help
Program Trees
qakbot_02390000.bin
Headers
.text
.rdata
.data
.rsrc
.reloc
.tdb
Program Tree
Symbol Tree
Imports
Exports
Functions
Labels
Classes
Namespaces
Filter:
Data Type Manager
Data Types
BuiltInTypes
qakbot_02390000.
windows_vs12_32
Filter:
Listing: qakbot.exe
00401a1b 50 PUSH EAX
Decompile: entry - (qakbot.exe)
1
/* same address */
AntiDebugSeekerPlugin [CodeBrowser: Demo:/qakbot.exe]
Edit Help
AntiDebugSeekerPlugin
Start Analyze
Display only the detection results
Detected Function List
FUN_0040352c
SetupDiGetDeviceRegistryPropertyA : 00403555
FUN_0040884d
GetLocalTime : 0040887b
FUN_00409c99
GetSystemTime : 00409ca4
FUN_00409881
SleepEx : 0040997d
FUN_004012f7
WaitForSingleObject : 00401347
FUN_004066b2
CreateThread : 004066c4
FUN_0040482a
GetThreadContext : 00404883
FUN_00404671
ResumeThread : 0040477a
FUN_0040385e
CloseHandle : 00403a6a
FUN_004033fc
VMware_I/O_port 0x5658 : 00403439
VMware_magic_value 0x564d5868 : 0040343d
VMware_magic_value 0x564d5868 : 00403472
FUN_0040349a
VMware_I/O_port 0x5658 : 004034d2
VMware_magic_value 0x564d5868 : 004034d6
FUN_0040330a
Environment_TimingCheck_CPUID CPUID : 00403319
FUN_0040336e
Environment_TimingCheck_CPUID CPUID : 004033ac
FUN_00404ded
CreateMutex_AlreadyExist : 00404e86
Unknown_Function
CreateMutex_AlreadyExist : 0040b178
CreateMutex_AlreadyExist : 0040b178
Code Unit
PUSH EDI
CALL dword ptr [->KERNEL32.DLL::...
Analysis Potential of Anti Debug API Analysis Environment Check : GetExitCodeProc... 00404f86
Analysis Potential of Anti Debug API Analysis Environment Check : GetSystemInfo 0040586e
Analysis Potential of Anti Debug API Analysis Environment Check : SetupDiEnumDevi... 004036ba
Analysis Potential of Anti Debug API Analysis Environment Check : SetupDiGetClass... 0040367f
Analysis Potential of Anti Debug API Analysis Environment Check : SetupDiGetDevic... 00403555
Analysis Potential of Anti Debug API Time Check : GetLocalTime 0040887b
Analysis Potential of Anti Debug API Time Check : GetLocalTime 00409123
Analysis Potential of Anti Debug API Time Check : GetLocalTime 0040921e
Analysis Potential of Anti Debug API Time Check : GetSystemTime 00409ca4
Analysis Potential of Anti Debug API Time Check : GetSystemTime 00409dc3
Analysis Potential of Anti Debug API Time Check : GetTickCount 0040560d
Analysis Potential of Anti Debug API Time Check : SleepEx 0040997d
Filter:
Console
Bookmarks
00401a28 entry PUSH EBP

The Analysis result of Ghidra-AntiDebugSeeker

```
if (bVar1) {
  uVar4 = FUN_004033fc(pCVar3,extraout_EDX);
  FUN_0040349a(extraout_ECX_00,(int)((ulonglong)uVar4 >> 0x20));
  FUN_004035b6();
  FUN_0040385e();
  FUN_00403bdf();
  FUN_00403d22();
  FUN_0040336e();
}
```

Anti Debug Codes

Only Return

Anti Debug Function	Detected / No Detected
FUN_4033fc	Detected (VM presence)
FUN_40349a	Detected (VM presence)
FUN_4035b6	Detected (Check Hardware)
FUN_40385e	Detected (File Operation)
FUN_403bdf	No Detected
FUN_403d22	No Detected
FUN_40336e	Detected (Environment_TimingCheck)

Introduction to Files related to the Ghidra version

Files Required to Run the Program

● Ghidra Script

AntiDebugSeeker.java

● Ghidra Extension

Ghidra_11.0.1_PUBLIC_AntiDebugSeeker.zip

◘ Configuration Files

anti_debug_Ghidra.config

anti_debug_techniques_descriptions_Ghidra.json

Summary

① Improve analysis efficiency.

② Custom rule files.

③ Further enhance debugging efficiency.

Thank you!

Github URL (IDA)

https://github.com/LAC-Japan/IDA_Plugin_AntiDebugSeeker

Thank you!

Github URL (GHIDRA)

https://github.com/LAC-Japan/Ghidra_AntiDebugSeeker

LAC